Volume 16, Issue 33      Atari Online News, Etc.      August 15, 2014

=~=~=~=



A-ONE #1633                                        08/15/14


~ NSA Eyed Preset Strikes! ~ People Are Talking!    ~ Reclassify Providers!
~ Call of Duty Multiplayer ~ Gamescom To Set Record ~ 3 New Xbox Bundles!
~ "BadUSB" Exploit Evil!   ~ More Facebook Concerns ~ Pop-up Ads Apology!

~ Mother & Son Fire Video! ~ Password Manager Sites ~ Share Games on PS4!

-* Chinn on Upcoming Atari Film *-
-* Net Neutrality Should Be Debated More *-
-* Apple Stores Users' Personal Data in China *-

=~=~=~=

->From the Editor's Keyboard                "Saying it like it is!"
  """"""""""""""""""""""""""""

Another week, more sagas - but I'll skip past all that in order to get
this week's issue out in a fairly timely fashion.  Afterall, there's
only so much time to vent frustration; and I have little this week.
Typical.

Until next time...

=~=~=~=

->In This Week's Gaming Section  - Three New Xbox Bundles!
  """""""""""""""""""""""""""""""    Why PS4 Will Let Players Share Games!
                                     'Call Of Duty: Advanced Warfare'!
                                     And much more!

=~=~=~=

->A-ONE's Game Console Industry News   -  The Latest Gaming News!
  """"""""""""""""""""""""""""""""""""

    Three New Xbox Bundles, Pre-loading Feature Announced at Gamescom

A trio of new retail bundles annouced for Xbox One will feature soccer
game "FIFA 15," sci-fi shooter "Call of Duty: Advanced Warfare" and
oddball zombie action title "Sunset Overdrive."

Speaking as part of the Xbox Media Briefing in Cologne, Germany, prior to
the opening of video game convention Gamescom, Microsoft representatives
introduced three new console bundles designed to make it easier for
consumers to choose an Xbox One this holiday season.

Both "Call of Duty: Advanced Warfare" and "FIFA 15," though available on
a multitude of consoles as well as on PC, will include exclusive hooks

for Xbox owners: first admission to the optional expansions of "COD: AW,"
and the returning FIFA Ultimate Team Legends mode, itself a fork of the
sports game's more widely available Ultimate Team player collection
spin-off.

By contrast, "Sunset Overdrive" is entirely exclusive to Xbox One,
developed by long-time PlayStation contractor Insomniac Games
("Ratchet & Clank," "Resistance" franchises).

The vibrant, irreverent post-apocalyptic action game invites players to
have a whale of a time while they're surviving a zombie onslaught caused
by contaminated fizzy pop.

With the "FIFA 15" bundle limited to European (read: football mad)
territories, both it and the white Xbox One of the internationally
available "Sunset Overdrive" package are to retail for $399 /  399 /
£349, while the "Call of Duty" themed bundle, with its custom colored
console and controller and cavernous 1TB hard drive, will go for $499 /
 499 / £429.

Closing the conference, Head of Xbox Phil Spencer revealed that "FIFA 15"
and "Call of Duty: Advanced Warfare" would be the first Xbox One titles
to allow both pre-order and pre-load via Xbox Live, a feature that has
already made its way onto PC and PS4; the mechanism allows players to get
going as soon as release day hits, having already completed the hefty
game data download.


 Why PS4 Will Let Players Share Games Without Swapping   Or Buying Discs


A panic among gamers was set off last year by rumors that the new consoles
from Sony and Microsoft would keep anyone but the original buyer of a game
from playing it. At risk was the time-honored tradition of swapping discs
among friends, not mention the sprawling market for used games. The
feared second-hand game restrictions didn t come to pass, and in the
months since, Sony has been developing an increasing number of ways to
play games without forking over $60 for a disc of your own.

A newly announced update to the PlayStation 4 software will allow players
to join in a friend s game online, even if the person joining doesn t
have a copy of the game. The idea, called Share Play, is basically a
virtual version of inviting someone over to sit next to you on the couch.

Share Play will be available in the fall. Sony also recently launched
Playstation Now, a streaming service that allows people to rent games for
far less than the retail price. Electronic Arts (EA), meanwhile, has its
own streaming service for XBox One that gives gamers access to a range
of titles for a monthly fee.

After hearing a lot about the anticipated death of console gaming in
recent years, the industry is clearly trying to be flexible about how
games can be purchased and played. That demise hasn t seemed quite as
imminent lately. Sony said Tuesday it has sold 10 million PS4 consoles,
easily beating the pace for its last generation of consoles. Microsoft
also had a press event Tuesday but didn t mention anything about sales,
so it s safe to assume that Sony remains comfortably ahead.

The business models for new forms of console gaming, however, could get

tricky. No matter the type of media, streaming services make content creators nervous, because such services dull the incentive to keep buying media through traditional methods. In theory, such features as PS4's Share Play could further discourage people to buy as many games.

Sony s not worried. It says that virtually any game that works on PS4 will be available for Share Play, with the exception of games that require the use of peripheral devices, such as a camera. At the moment, the company sees the feature purely as a way to help get gamers excited about games they don t own, says John Koller, Playstation s head of marketing. Sony is just leaving its options open for different business models in the future.

Game developers will also have the option to write code that keeps the feature from working, but Koller says he doesn t know of any who plan to do so. He predicts developers won t see Share Play as any more threatening than old-fashioned disc sharing. There is a sensitivity to sharing discs, because you can complete the game that way, he says. This way, you get a taste. To get the full meal you have to buy the game.

David Edery, the chief executive of Spry Fox, whose game Road Not Taken was recently released for PS4, said he s excited for Share Play, mostly because it mimics the way he played games as a kid. Sony has a vested interest in making sure games keep selling, he says. Bear in mind that the Playstation division generates nearly all its profit from games, not hardware.

Games Fair To See Record Visitors on Microsoft, Sony Ware

The world s largest video-game fair is set to draw a record attendance this week as visitors seek out titles for new consoles from Microsoft Corp. and Sony Corp.

Gamescom, which starts today in Cologne, Germany, is expected to draw more visitors than last year s 340,000, organizers say. For the event, Sony tapped veteran game developer Hideo Kojima to promote the latest installment of Metal Gear Solid, one of the best-selling series in history, for its PlayStation 4.

Microsoft is showing footage of Quantum Break, an Xbox One-exclusive action adventure. Among games publishers, Ubisoft Entertainment will compete with Activision Blizzard Inc. and Electronic Arts Inc. in getting a head start into the holiday season and benefit from surging sales of the latest machines.
Story: A Shortcut to Cure Big Data Headaches

The next-generation consoles are selling better than expected, but there is a dearth of games tailored to what they re capable of, Todd Mitchell, an analyst at Brean Capital LLC in New York, said in a phone interview. We re finally looking at a much more robust lineup for the fall, and there will start to be winners and losers.

Unlike the Electronic Entertainment Expo in Los Angeles, Gamescom, which has been held since 2009, is open to the public on four out of five days, making it more important to create resonance on social media such as Twitter Inc. and Facebook Inc.

To win new customers, games makers are trying out new business models, such as the sort of monthly subscriptions used by Netflix Inc., instead of the traditional pay-per-game model. At the same time, they need to keep an eye on smaller publishers winning users over with free-to-play games that generate revenue through payments for in-game content such as upgrades to weapons.

Sony s new console has sold 10 million units worldwide, the Tokyo-based company said at a news conference yesterday. The machine has been leading Microsoft s Xbox One since the two devices started selling in late 2013. That s prompted Microsoft to offer its console unbundled from the Kinect motion-sensing device to lower its sales price.

 We ll be there in a big way,  Alan Lewis, vice president of corporate communications at Take-Two Interactive Software Inc., said in a telephone interview.

The New York-based company will be letting users play planned releases, including NBA 2K15 and WWE 2K15 that will be on sale in October for new-generation consoles and PCs. Professional wrestler Big Show will appear on behalf of the company, to deliver a  special announcement about WWE 2K15, Lewis said.

Electronic Arts, the largest maker of games for the Xbox One and PS4, will present playable versions of its sports titles FIFA 15 and NHL 15, and will also show role-playing game Dragon Age Inquisition along with mobile titles, Chief Operating Officer Peter Moore said in an interview.


'Call Of Duty: Advanced Warfare' Multiplayer Revealed


Call of Duty: Advanced Warfare promises big changes to Activision s yearly franchise, and nowhere is this more apparent than the game s multiplayer mode.

The new exoskeleton adds numerous new movement options, including boost jump, dodge, slide, and slam. The first truly futuristic Call of Duty promises more verticality in map design, reminiscent of Respawn s recent Titanfall shooter with its mechs and double-jumping pilots, though developer Sledgehammer was developing its game at the same time as Respawn.

Multiplayer also expands on customization options, with Activision promising nearly 350 custom weapons, over 1,000 in-game player rewards, and over 2 billion unique player combinations. I m not sure if that s overboard, but at least we have choices.

 With Call of Duty: Advanced Warfare we introduced the first new lead developer to the franchise in a decade and our first three-year development cycle, with one mission: bring breakthrough innovation to the franchise, while also honoring its roots.  We feel Sledgehammer Games has risen to that challenge,  Activision Publishing, Inc. s CEO, Eric Hirshberg said in a statement.   Advanced Warfare introduces significant new mechanics to multiplayer that truly changes the game, but more importantly just speaking as a gamer it s a hell of a lot of fun.

Other changes include the evolution of the Pick 10 system upping this to

Pick 13; co-op scorestreaks; and a new energy class of weapons. These futuristic weapons use heat management rather than ammo, though Sledgehammer has gone to great lengths to make sure that even the science fiction elements of Advanced Warfare are plausible. , from weapons to the exoskeletons.

Players will also be able to test out their arsenal in a new virtual shooting range, and a Virtual Lobby to show off your custom characters and rewards.

Character customization itself has been overhauled pretty radically, allowing gamers to use the new Create-an-Operator system to customize a wide array of items from shirts to glasses to the exoskeleton itself. Sledgehammer has also introduced Supply Drops which drop random in-game items including weapons and other gear and fall more frequently the more you play.

New game modes such as Uplink a sort of rugby-esque twist on capture the flag involving a satellite drone and Momentum have also been added.

All told there are a lot of big changes coming to Advanced Warfare s multiplayer (and single player) mode, quite possibly the biggest suite of changes and innovations since Modern Warfare. This is both exciting for those of us who ve been asking for more innovation and a bit of a risk for Activision and Sledgehammer.

Call of Duty is still the top dog, and I think bringing innovation to the table is the only way to stay number one. On the other hand, the old maxim If it ain t broke, don t fix it also applies. And Call of Duty fans have not always responded positively to attempts at change.

Still, it s exciting to see the video game industry s biggest franchise offer up some new and much-needed twists. Better to take risks than to slumber in mediocrity.


PSP Ends Shipments in Japan


Sony Computer Entertainment Japan announced on Monday that it will cease production of new Japanese PlayStation Portable (PSP) units in June. A little under ten years have passed since the portable video game system debuted in Japan.

The company's Sony Store began a campaign on Tuesday titled Summer 2014 Super Coaxing Strategy! which will allow PSP-3000 owners to turn in their old PSP system and get 3,000 yen (about US$30) off the purchase of a PlayStation Vita system. In addition, PSP-2000 and PSP go owners will get an 1,000 yen (about US$10) discount. Students will get an increased discount of 1,000 yen more off.

Sony released its first portable game system in Japan on December 12, 2004. As of January 2013, the system has sold 19.26 million units in Japan, and has sold 69 million units worldwide. Multiple titles are scheduled for release for the system later this year, including two QuinRose titles. Otomate's Urakata Hakuoki: Akatsuki no Shirabe PSP game is scheduled to ship on August 7.

```
                                =~=~=~=
```

                    Documentary Director Chinn on Upcoming Atari Film


Video games have gone Hollywood, but a new documentary recalls those
early, halcyon days when a technology startup called Atari first brought
the arcade experience into the living room more than three decades ago.

Many fans and serious gamers may not know the back story of how it all
began, boomed, and crashed-before many of them were born-or that some of
the biggest stars in Silicon Valley had humble beginnings creating code
and cartridges for Atari.

Then there s the unearthing last year of thousands of E.T. game
cartridges widely considered one of the worst games ever- in a New Mexico
landfill.  The games were unceremoniously buried under cover of darkness,
providing enough intrigue to ensnare a pair of multiple-award winning
documentarians wanting to tell that tale as well.

Emmy winning producer Jonathan Chinn and his cousin, double-Oscar winner
Simon Chinn, and their LIGHTBOX media company are the driving force
behind the documentary series and its first film:  Atari: Game Over.

The doc will premiere  in fall  and will be distributed by Microsoft via
its Xbox game console; apropos since the software giant embodies the
growth and symbiotic relationship between video gaming and the tech
revolution.

In an exclusive interview with FOX Business, Jonathan Chinn shared his
view on how Atari changed his life, and likely yours, forever and
deserves its place as tech revolutionary rabble-rouser

What drew you to the Atari story?

It was the first entertainment-based Silicon Valley company, and there s
the epic fail (of Atari) and video game crash.  It struck us as we hit
upon something that would allow us to look at a moment in time through
an intriguing, slightly controversial story.

This series (of documentary films) is about seminal and slightly
underexposed moments in the digital revolution.  When the story came to
our attention, I think our first instinct was to think it was a bit of a
niche story appealing to gamers. We want the series as a whole to appeal
to a broader audience.

While the burial of  ET  cartridges may not stack up against the
formation of Apple or Facebook in seminal moments of the digital
revolution   I think Atari has a place in that evolution.  They don t
exist today, yet they were there before everybody else.  Steve Jobs
worked there, Steve Wozniak worked there.  You can trace back the
dot-com boom and philosophy, Atari started all of that, the

pot-smoking, geek chic revolution.

(Chinn takes a dramatic pause) The short answer, it was just a really damn good story.  Ultimately we re interested in good stories.

Did you have an Atari 2600 video game console?

I absolutely had the first generation Atari 2600.  I remember the day my father brought it back to the house on a weekend.  It was probably the most exciting moment in my life at that point.  That was another contributing factor to produce the film.  I m not a gamer, I haven t identified with the hard-core gaming community, but I was a gamer back then.  I remember the liberation of having an entertainment system in my house.

My relationship with the digital revolution could be traced back to then.  We had it before our first PC.

Have video games truly crossed into mainstream America?

I recently got an Xbox and haven t played a game since the 2600.  It s changed an enormous amount Technology is making video games feel in some ways more like movies.  It s a renaissance, the interest in Atari and our film show(s) renewed interest and respect for the video game creator as an artist.  The existing boundaries between art and gaming, or film and gaming are getting broken down.  The big show runners, filmmakers, all play games: Joss Whedon, J.J Abrams they re coming out of the digital closet.

Were you surprised that Microsoft s Xbox hired LIGHTBOX to produce documentaries?

We re living in digital world.  The revolutionary part has happened. It s time to do a series that asks the question:   How did we get here? And,  What does it mean for where we re heading?

We thought about who would be interested, and we felt strongly it should be a company that s part of that (tech revolution)- Amazon.com, Netflix), Hulu, and until recently, Xbox (Microsoft has essentially shut down its Xbox Entertainment Studios as part of recent, sweeping job cuts), we felt it was a great fit.

How many docs will you produce for Xbox?

I can t answer that, with the closure of Xbox Studios, it s uncertain. We have two films including  Atari  that are close to being done.

The other film is a very different story.  Greg Barker (who directed the  Manhunt  HBO documentary on the hunt for Usama bin Laden) is making a film about the role of citizen journalism in the hours and days after the Boston Bombings.  It s about Reddit and the rush to judgment and the digital and social media witch hunt that went on, mostly for wrong people.  It celebrates citizen journalism and asks:  Should there be boundaries for journalism so things like this won t happen?   There s no release date-sometime in the next four to six months.

=~=~=~=

FCC Commissioner In Columbus Says Net Neutrality Should Be Fully Debated


The Federal Communications Commission is preparing to collect public comment on a controversial proposal to create what many call a web superhighway.

"My own view is that the FCC should prioritize polices that make broadband available to everybody," said FCC commissioner Ajit Pai. "That includes rich and poor, urban and rural.  If we do that I'm sure the net neutrality concerns will evaporate."

Pai will be just one of just five commissioners voting on the issue.  He sat down with 10TV today and said his agency has so far received more than one million comments on the web issue.

And it's not over yet.

"Whatever regulations the FCC adopts it's important to remember it's going to be embroiled in litigation for potentially years," said Pai.

Many web users are adamantly opposed to the idea.

"I think it's a very dangerous precedent," said social media expert Kelley Bell.  "Imagine roads and only the big companies can use the freeways and the rest of us drive in the ally's and nobody is fixing the potholes.  That's what people are afraid of."

So afraid that earlier this year hundreds of protesters rallied outside the Federal Communication Commission in Washington.

"This is the first time in the history of the world that the people have had equal access to information," said Bell.  "And the ability to speak and be heard. We have to protect that."

The FCC proposal sparked a lot of criticism for allowing providers like AT&T and Verizon to charge companies for a superhighway.

The agency is now in the middle of a 90 day review.

Bell says that's why many web users want the FCC to slow down and take a lot of public comment.  "The internet moves at the speed of light," said Bell.  "But our lawmaking in regards to it needs to take its time."


Reclassify Internet Providers for 'Net Neutrality'


US regulators' new "net neutrality" rules should classify internet providers more like public utilities to prevent them from potentially slowing users' access to some web content, the New York Times said in an

editorial.

The statement comes as the Federal Communications Commission (FCC) is preparing to set the new rules, which would regulate how internet service providers, or ISPs, manage traffic on their networks. In January, a federal court struck down the agency's previous version of those rules.

The FCC is now collecting public comment on the rules it tentatively proposed in May, which the New York Times called troubling.

While prohibiting ISPs from blocking any content, the proposal suggested allowing some "commercially reasonable" deals where content companies, such as Netflix Inc or Amazon.com Inc, could pay ISPs, such as Comcast Corp or Verizon Communications Inc, to ensure smooth and fast delivery of their web traffic.

Although FCC Chairman Tom Wheeler has insisted the agency would carefully guard against abuse of the rules, the proposal drew ire from public interest groups and large Web companies. They say it would result in faster download speeds for some content as other data would be relegated to "slow lanes."

Consumer advocates have called on the FCC to instead reclassify ISPs as telecommunications services rather than as the less-regulated information services they are now, saying the move would give more power to the FCC to stop potential violators of net neutrality.

The New York Times has now joined their ranks, pointing to President Barack Obama's recent comments at a recent conference with African leaders in Washington, where he said an equally accessible Internet is important for "the next Google or the next Facebook."

The New York Times editorial said, "Small and young businesses will not be able to compete against established companies if they have to pay fees to telephone and cable companies to get content to users in a timely manner."

A better option, the paper said, would be for the FCC to reclassify broadband Internet service as a telecommunications service, which would allow the regulators to prohibit ISPs from "engaging in unjust or unreasonable discrimination against content."

Experts have disagreed on whether or how reclassification would adequately prevent pay-for-priority deals.

ISPs and Republicans, both in Congress and at the FCC, strongly oppose reclassification, saying a heavier regulatory burden may hurt investment in broadband networks.

The ISPs also say they support an open internet and having some content in "slow lanes" would upset their customers and so is not in their interest.

Wheeler has not proposed reclassification as the solution, but has not taken it off the table as a potential route.

NSA Eyed Preset Strikes in Cyberattacks

The National Security Agency secretly planned a cyberwarfare program that could automatically fire back at cyberattacks from foreign countries without any human involvement, creating the risk of accidentally starting a war, according to a new report based on interviews with former NSA contractor Edward Snowden.

The program, codenamed MonsterMind, would have let the military agency automate the process of "hunting for the beginnings" of a foreign cyberattack, the report said. The software would be constantly on the lookout for digital "traffic patterns" that indicated known or suspected attacks, the report published this week by Wired magazine said.

The report, part of a wide-ranging interview with Snowden in Moscow, described the MonsterMind program as "in the works" and went further than other programs that existed for decades. Without any human involvement, Snowden told the magazine, a counter-attack could be leveled at an innocent party    largely because initial attacks are often routed or diverted through other countries.

"You could have someone sitting in China, for example, making it appear that one of these attacks is originating in Russia. And then we end up shooting back at a Russian hospital," Snowden said. "What happens next?"

The problem of attribution after a cyberattack has long unsettled computer security experts. A House technology subcommittee in 2010 concluded that, "proactively tracing interactions within a system may help determine where an attack originated after one occurs, but tracing every interaction is impractical and quite likely unconstitutional."

Snowden also called the program a major threat to privacy because NSA would first "have to secretly get access to virtually all private communications coming in from overseas to people in the U.S.," said the new report, by NSA expert and author James Bamford.

Snowden remains exiled in Russia since leaking top secret NSA documents to journalists last year. They revealed the NSA was collecting the phone records and digital communications of millions of citizens not suspected of a crime, prompting congressional reform.

The NSA declined to comment on specifics of the Wired report. A spokeswoman, Vanee Vines, instead said: "If Mr. Snowden wants to discuss his activities, that conversation should be held with the U.S. Department of Justice. He needs to return to the United States to face the charges against him."

Snowden is charged under the U.S. Espionage Act and faces up to 30 years in prison for leaking the documents.

The U.S. government has elevated lately the damages of foreign cyberattacks against American interests. In May, the Justice Department brought first-of-its kind cyber-espionage charges against five Chinese military officials accused of hacking into U.S. companies to gain trade secrets.

Snowden also told the magazine that the NSA tried to hack into a major Syrian Internet router in 2012 during the middle of the country's civil war. But he said the NSA mistakenly "bricked" the router    computer-speak for rendering it useless    temporarily crippling Internet access there.

Apple Begins Storing Users' Personal Data on Servers in China

Apple Inc has begun keeping the personal data of some Chinese users on servers in mainland China, marking the first time the tech giant is storing user data on Chinese soil.

The storage of user data in China represents a departure from the policies of some technology companies, notably Google Inc , which has long refused to build data centers in China due to censorship and privacy concerns.

Apple said the move was part of an effort to improve the speed and reliability of its iCloud service, which lets users store pictures, e-mail and other data. Positioning data centers as close to customers as possible means faster service.

The data will be kept on servers provided by China Telecom Corp Ltd, the country's third-largest wireless carrier, Apple said in a statement on Friday.

"Apple takes user security and privacy very seriously," it said. "We have added China Telecom to our list of data center providers to increase bandwidth and improve performance for our customers in mainland china. All data stored with our providers is encrypted. China Telecom does not have access to the content."

A source with knowledge of the situation said the encryption keys for Apple's data on China Telecom servers would be stored offshore and not made available to China Telecom.

Apple has said it has devised encryption systems for services such as iMessage that even Apple itself cannot unlock. But some experts expressed scepticism that Apple would be able to withhold user data in the event of a government request.

"If they're making out that the data is protected and secure that's a little disingenuous because if they want to operate a business here, that'd have to comply with demands from the authorities," said Jeremy Goldkorn, director of Danwei.com, a research firm focused on Chinese media, internet and consumers.

"On the other hand if they don't store Chinese user data on a Chinese server they're basically risking a crackdown from the authorities."

Goldkorn added that data stored in the United States is subject to similar U.S. regulations where the government can use court orders to demand private data.
A spokesman for China Telecom declined to comment.

With its rising middle class, China has become an increasingly important market for Apple. Sales of the iPhone rose almost 50 percent in China in the three months ended June and salvaged an otherwise lackluster quarter for the Cupertino company.

Other companies have opted not to situate servers in China, where they would have to comply with local laws.

Google publicly abandoned China in 2010 and moved its services, including its search engine, to Hong Kong-based servers after refusing to comply with Chinese government censorship. Microsoft Corp also does not have servers for its email service in China.

Yahoo Inc came under criticism in 2005 after it handed to Chinese authorities emails that led to the imprisonment of Shi Tao, a journalist who obtained and leaked an internal censorship order the government had sent Chinese media.

"China doesn't want any digital service offered to Chinese people to be hosted offshore," said Goldkorn. "I suppose it was inevitable that Apple had to comply if they were using foreign servers for Chinese user data."

In July, Apple's iPhone was branded a danger to China's national security by state media, because of the smartphone's ability to track and time-stamp user locations. Apple denied tracking user locations.

Apple has frequently come under fire from Chinese state media, which accused the company of providing user data to U.S. intelligence agencies and have called for 'severe punishment'.

The U.S. company has strongly denied working with any government agencies to create back doors into its products or servers. "We have also never allowed access to our servers. And we never will," Apple has previously stated.

News of the China Telecom deal emerged Thursday after a local government website in the southeastern province of Fujian announced that iCloud had migrated to China Telecom's servers after 15 months of rigorous testing and review. The website article is no longer available on the site.


This Thumbdrive Hacks Computers.  BadUSB  Exploit Makes Devices Turn  Evil


When creators of the state-sponsored Stuxnet worm used a USB stick to infect air-gapped computers inside Iran's heavily fortified Natanz nuclear facility, trust in the ubiquitous storage medium suffered a devastating blow. Now, white-hat hackers have devised a feat even more seminal an exploit that transforms keyboards, Web cams, and other types of USB-connected devices into highly programmable attack platforms that can't be detected by today's defenses.

Dubbed BadUSB, the hack reprograms embedded firmware to give USB devices new, covert capabilities. In a demonstration scheduled at next week's Black Hat security conference in Las Vegas, a USB drive, for instance, will take on the ability to act as a keyboard that surreptitiously types malicious commands into attached computers. A different drive will similarly be reprogrammed to act as a network card that causes connected computers to connect to malicious sites impersonating Google, Facebook or other trusted destinations. The presenters will demonstrate similar hacks that work against Android phones when attached to targeted computers. They say their technique will work on Web cams, keyboards, and most other types of USB-enabled devices.

"If you put anything into your USB [slot], it extends a lot of trust," Karsten Nohl, chief scientist at Security Research Labs in Berlin, told Ars. "Whatever it is, there could always be some code running in that

device that runs maliciously. Every time anybody connects a USB device to your computer, you fully trust them with your computer. It's the equivalent of [saying] 'here's my computer; I'm going to walk away for 10 minutes. Please don't do anything evil."

In many respects, the BadUSB hack is more pernicious than simply loading a USB stick with the kind of self-propagating malware used in the Stuxnet attack. For one thing, although the Black Hat demos feature only USB2 and USB3 sticks, BadUSB theoretically works on any type of USB device. And for another, it's almost impossible to detect a tampered device without employing advanced forensic methods, such as physically disassembling and reverse engineering the device.

Antivirus scans will turn up empty. Most analysis short of sophisticated techniques rely on the firmware itself, and that can't be trusted.

"There's no way to get the firmware without the help of the firmware, and if you ask the infected firmware, it will just lie to you," Nohl explained.

Most troubling of all, BadUSB-corrupted devices are much harder to disinfect. Reformatting an infected USB stick, for example, will do nothing to remove the malicious programming. Because the tampering resides in the firmware, the malware can be eliminated only by replacing the booby-trapped device software with the original firmware. Given the possibility that traditional computer malware could be programmed to use BadUSB techniques to infect any attached devices, the attack could change the entire regimen currently used to respond to computer compromises.

"The next time you have a virus on your computer, you pretty much have to assume your peripherals are infected, and computers of other people who connected to those peripherals are infected," Nohl said. He said the attack is similar to boot sector infections affecting hard drives and removable storage. A key difference, however, is that most boot sector compromises can be detected by antivirus scans. BadUSB infections can not.

The Black Hat presentation, titled BadUSB on accessories that turn evil, is slated to provide four demonstrations, three of which target controller chips manufactured by Phison Electronics. They include:

Transforming a brand-name USB stick into a computer keyboard that opens a command window on an attached computer and enters commands that cause it to download and install malicious software. The technique can easily work around the standard user access control in Windows since the protection requires only that users click OK.

Transforming a brand-name USB stick into a network card. Once active, the network card causes the computer to use a domain name system server that causes computers to connect to malicious sites impersonating legitimate destinations.

Programming a brand-name USB stick to surreptitiously inject a payload into a legitimate Ubuntu installation file. The file is loaded onto the drive when attached to one computer. The tampering happens only after it is plugged into a separate computer that has no operating system present on it. The demo underscores how even using a trusted computer to verify the cryptographic hash of a file isn't adequate protection against the attack.

Meet badBIOS, the mysterious Mac and PC malware that jumps airgaps
Like a super strain of bacteria, the rootkit plaguing Dragos Ruiu is
omnipotent.

The capabilities of BadUSB closely resemble the mysterious badBIOS
malware security consultant Dragos Ruiu said repeatedly infected his
computers. Nine months after Ars reported security researchers were
unable to independently reproduce his findings, that remains the case.
Still, Nohl said BadUSB confirms that the badBIOS phenomena Ruiu
described is technically feasible.

"Everything Dragos postulated is entirely possible with reasonable
effort," Nohl said. "I'm pretty sure somebody is doing it already. This
is something that's absolutely possible."

Nohl said there are few ways ordinary people can protect themselves
against BadUSB attacks short of limiting the devices that get attached to
a computer to those that have remained in the physical possession of a
trusted party at all times. The problem, he said, is that USB devices
were never designed to prevent the types of exploits his team devised.
By contrast, peripherals based on the Bluetooth standard contain
cryptographic locks that can only be unlocked through a time-tested
pairing process.

The other weakness that makes BadUSB attacks possible is the lack of
cryptographic signing requirements when replacing device firmware. The
vast majority of USB devices will accept any firmware update they're
offered. Programming them in the factory to accept only those updates
authorized by the manufacturer would go a long way to preventing the
attacks. But even then, devices might be vulnerable to the same types of
rooting attacks people use to jailbreak iPhones. Code signing would
likely also drive up the cost of devices.

"It's the endless struggle between do you anticipate security versus
making it so complex nobody will use it," Nohl said. "It's the struggle
between simplicity and security. The power of USB is that you plug it in
and it just works. This simplicity is exactly what's enabling these
attacks."


Facebook's New Ad Tracking Raises Privacy Concerns


Facebook will move deeper into advertising analytics and begin tracking
information between devices and sharing it with advertisers. It's a move
that promises to upset Facebook users with privacy concerns and make the
world's largest social networking site boatloads of money, Bloomberg
reports.

The plan is the latest in a line of tactics that have made Facebook,
which reached nearly $3 billion in revenue in the second quarter, an
extremely profitable marketing tool. It's also helped build its
controversial reputation among a number of critics as a Big
Brother-esque corporate spying tool.

Users sign into Facebook on multiple devices such as phones, tablets,
laptops and desktops. Facebook already tracks how many times a user
clicks on each ad, but it can now tell how often a user clicks an ad on

their phone versus how many times using a desktop. It can also track which of those visits lead to purchases.


## Woman Accused of Helping Son Set Himself on Fire for Facebook Video

A North Carolina woman is accused of helping to record her teenage son set himself on fire after he doused his body with fingernail polish as part of a social media stunt, police said.

Janie Lachelle Talley, 41, watched as her 16-year-old son attempted to complete a  fire challenge  video for Facebook on July 29, the Charlotte-Mecklenburg Police Department said Monday. The boy suffered minor burns on his chest and neck.

The video showed others putting out the fire.

 The mother of the victim was present and aware of what her son [was] doing and facilitated the recording,  a police statement said.

Police arrested Talley on Aug. 6 and charged her with contributing to the delinquency of a juvenile, according to the statement.

The  fire challenge  has been spreading on social media with people pouring flammable liquids on themselves, lighting it, trying to quickly extinguish the fire, and then posting a video online.


## This Story Probably Won t Make You Change Your Passwords

What s a three-word formula for procrastination?  Change your passwords.  We were told that back in April, when the Heartbleed vulnerability led to widespread calls to change all our passwords   except for the ones that didn t need changing. We re now hearing it again after Hold Security s vague report of the theft of 1.2 billion logins by  CyberVor  Russian criminals.

Not long after Heartbleed, a flaw that could allow attackers to steal logins from thousands of allegedly secure websites, my colleague Rafe Needleman suggested that we schedule a holiday just to change our passwords.

Maybe that would make a difference? Because, so far, not much else has.

A password-manager site s users: Meh?You might think people who already trust a password-manager service like Dashlane to save logins too complex for mere human memory would be among the first to swap out their passwords. But you d be wrong. Only 29 percent of Dashlane s stored passwords were changed in the month after Heartbleed broke, marketing manager Ryan Merchant reported.

That represented a significant increase from the 21 percent of Dashlane passwords changed in the prior month, but nowhere near the  Change all the passwords!  sermons being delivered at the time.

What about CyberVor? Merchant wrote that 17 percent of passwords stored

with the New York- and Paris-based firm were changed in the five days
after that report, versus 21 percent in the five days after Heartbleed s
appearance.

Another password-management service, Personal, couldn t tell me how many
of its passwords were changed, because it doesn t track how and when its
users change their data at all. But the founder of this D.C.-based firm,
Shane Green, had a pretty good hunch about how many of his customers had
bothered: very few.

 Sites don t make it easy or consistent for users to reset passwords,
Green wrote in an email.  As someone who does change passwords regularly,
it takes way too much effort.

Don t panic?Going in and resetting every password every time you see
another report of a widespread data breach might not be such a good idea
anyway, especially if your haste leads you to pick passwords that are too
short or too easily guessed. (Meanwhile, picking a strong password is
getting even harder; the bad guys are catching up to the tactic of
stringing together unrelated words, as Ars Technica s Dan Goodin noted
Sunday.)

And what if the data-breach report itself has holes? Hold Security s
claims have received a skeptical hearing, thanks to its failure to offer
even hints about what companies or services were involved, not to mention
Hold s intention to charge people for access to the data.

Companies can sign up for a notification service starting at $120 a year,
but Hold s site doesn t say what its personal identity-protection service
would cost. Forgive me if that sales pitch doesn t have me breathless
with anticipation.

My old Washington Post colleague Brian Krebs vouched for Hold s methods
in a blog post (as you might expect, since he and founder Alex Holden
have worked together before), but he doesn t have much company at the
moment. Veteran cryptographer Bruce Schneier s conclusion:  This story is
getting squirrelier and squirrelier.

Hold Security s hometown paper, the Milwaukee Journal Sentinel, caught
Holden saying he had earned an engineering degree when he did not
graduate. Reporters Rick Romell and Bill Glauber spoke to two security
consultants who questioned Holden s marketing as  suspicious  or
 confrontational.

Hold Security didn t respond to a query sent through its website Sunday.

What you should do?Schneier s post ended with an observation about the
absence of  massive fraud or theft.  For that matter, Heartbleed has yet
to uncork a flood of account hijackings five months after its public
discovery.

To me, the best explanation for that lies in a word Schneier is fond of
throwing around: resilience. The Internet keeps working because parts of
it can break without taking others offline, courtesy of both its basic
architecture and the diversity of software on it.

You can and should put that principle to work in your own online life.
Here s a three-step process for doing that:

1. Identify the accounts you can least afford to see compromised: the

email account that helps you log in to other sites (where your password recovery emails are likely to be sent), and the social-media account that people trust to be the real, offline you.

They re the most tempting targets for an attacker, because each can enable so much other theft. Turn on two-step verification   where you vouch for a login by entering a one-time code sent as a text message or computed automatically by an app on your phone   and a password compromise alone won t be able to capture those accounts.

If a mail service   say, the one provided by your Internet provider   doesn t offer that option, then it s time to consider making a switch. Two-step verification will do far more to protect you than crafting a complex password.

2. Spread your business around. Intentionally balkanizing your online and financial services does create more work for you   here s where using a password manager like Dashlane, LastPass, or Personal s Fill It helps   but it also lowers the potential damage from having any one account compromised.

In that respect, I m glad Facebook gave up on trying to replace email: It makes the site less of a single point of failure.

3. Try to reduce the amount of data at risk at any one site. You can do some of this yourself   do you really need to have your credit card stored at so many online retailers? But you ll probably have to wait and hope that the sites you use on a regular basis will drop the habit of storing all the data they possibly can about you, on the off chance it might come in handy one day.

We, in turn, will have to trust some sites to build detailed profiles of our usage so that they can spot a suspicious login in time, just as we trust credit-card companies to spot sketchy transactions today. There s sadly no other way, not least when we can t count on users to pick good passwords or to activate two-step verification.

If all of this looks like a recipe for muddling through: Yes, it is. Muddling through got the Internet off the ground in the first place. It also got us through the Year 2000 bug, and it isn t yet exhausted as a formula for keeping the online world working, more or less.


                    Man Who Invented Pop-Up Ads: 'I'm Sorry'


Ethan Zuckerman is sorry.

Zuckerman, who leads the Center for Civic Media at MIT, says he didn t realize what he was bringing into the world when he wrote the code for the first pop-up ad more than 20 years ago.

He tells the story of how it happened in an exquisite essay about how the ad-based business model came to dominate the Internet and why it really shouldn t (and what we ought to do about it).

It was the mid-1990s, and Zuckerman was working as a designer and programmer for Tripod.com:

"At the end of the day, the business model that got us funded was advertising. The model that got us acquired was analyzing users personal homepages so we could better target ads to them. Along the way, we ended up creating one of the most hated tools in the advertiser s toolkit: the pop-up ad.

It was a way to associate an ad with a user s page without putting it directly on the page, which advertisers worried would imply an association between their brand and the page s content. Specifically, we came up with it when a major car company freaked out that they d bought a banner ad on a page that celebrated anal sex. I wrote the code to launch the window and run an ad in it. I m sorry. Our intentions were good.

When Geocities introduced pop-ups a few weeks later, he says, they reused his code.

"Not only did I deploy what was probably the first popup, I wrote the javascript and the server-side Perl to launch it," Zuckerman told me in a follow-up. "I m old."

## Microsoft Employees 'Suggested Internally' To Change Internet Explorer's Name Distancing It From Previous Bad Rap

During an "Ask Me Anything" chat session at Reddit yesterday, Internet Explorer's developers took to answering a bunch of questions from their adoring fans. Well - "adoring" might not be the best word. Judging by the thread's title, "We build Internet Explorer. I know, right?", it's almost like the developers knew that a can of worms was about to be opened.

While the Reddit thread contained its expected share of haters and trolls, a couple of great questions were asked, such as the one from user asianorange, "How you ever consider rebranding and changing the name of Internet Explorer?"
The response might strike some as a little surprising: "It's been suggested internally; I remember a particularly long email thread where numerous people were passionately debating it. Plenty of ideas get kicked around about how we can separate ourselves from negative perceptions that no longer reflect our product today."

User codecracker25 then followed-up with a question of why a name change never actually happened, given the discussions. The devs then responded, "The discussion I recall seeing was a very recent one (just a few weeks ago). Who knows what the future holds :)

If a name change is something that Microsoft has discussed in the past, and has once again in the past month, it does lead me to believe that it's something that's fairly likely to happen. As it is today, Internet Explorer isn't a "bad" browser - a lot of work has gone into the software in recent years to make sure that's now the case. Given its momentum, it could even be a serious contender in the years ahead.

But to a lot of people, that simply doesn't matter. IE is still a laughing stock, and most well-versed Windows users wouldn't ever think of using it. It seems that most who do aren't the type to go search around for alternatives, or simply stick with it because it works for them. Why change if it works for you?

I personally think renaming the browser would be a smart thing for Microsoft to do, but it's obvious that it's a decision that can't come lightly. IE is a very integral name within the Windows brand, so to completely replace that name would be nothing short of major. It'd be almost as major as Microsoft renaming Windows itself.

What do you guys think? Should Microsoft suck-it-up and try to make people forget about the past by making Internet Explorer the best it can be? Or should it take the easy way out and rename it?


=~=~=~=